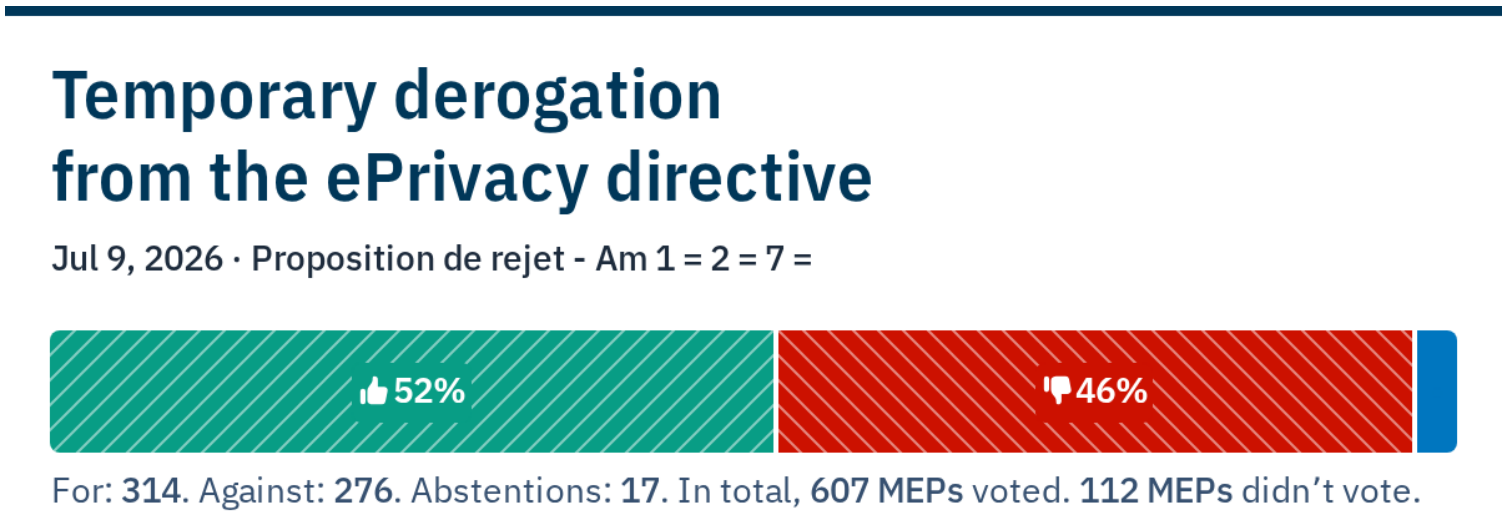
CHAT CONTROL 1.0

«What really happened on 9 July with Chat Control 1.0? The European Parliament approved the revival of the temporary derogation (Chat Control 1.0 / EU Regulation 2021/1232) that expired on 3 April 2026. **CHAT CONTROL 1.0 HAS NOT BECOME LAW.»**

REGULATION (EU) 2021/1232 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 July 2021

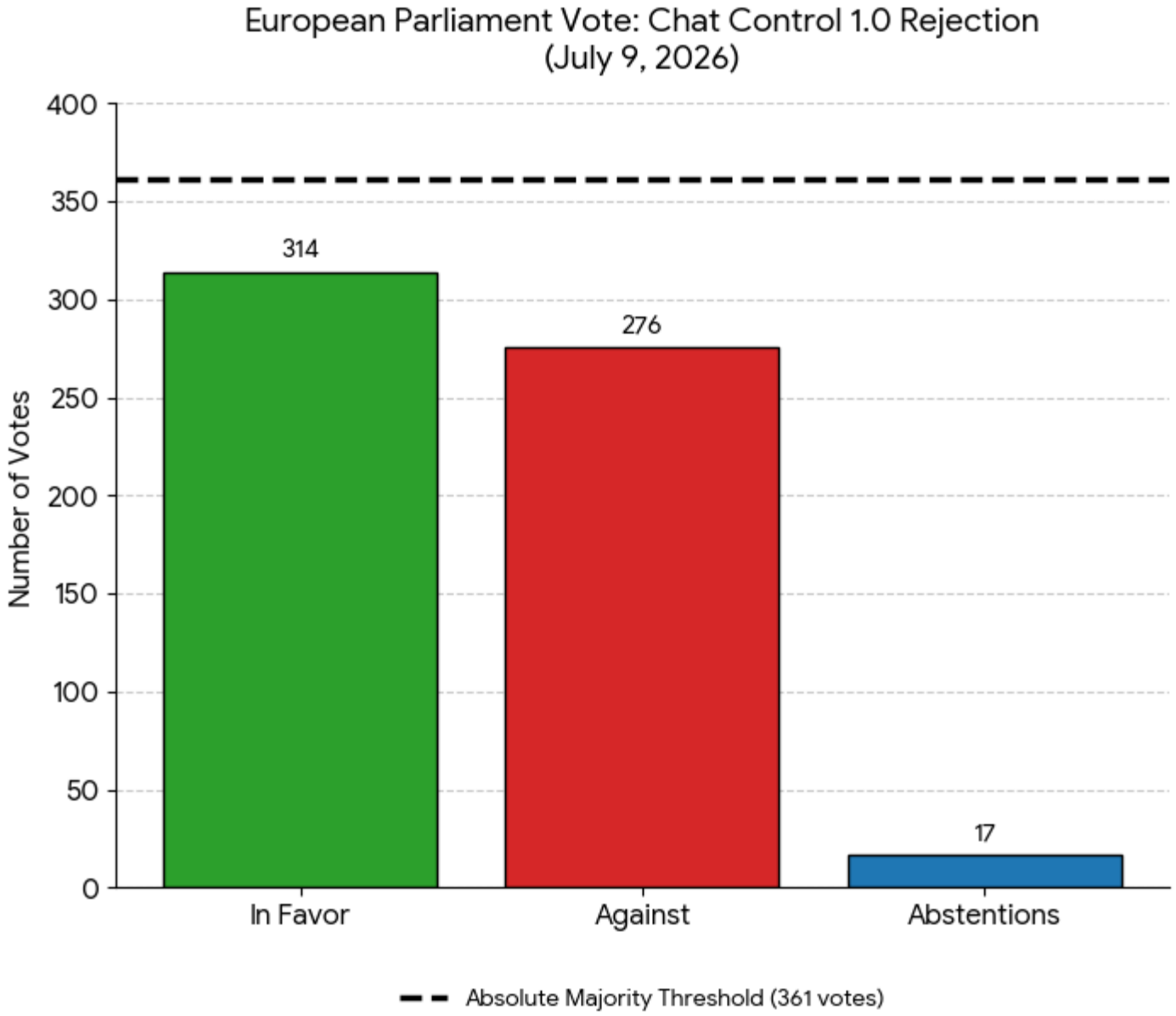
on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse



PART 1 – CHAT CONTROL 1.0 – WHAT REALLY HAPPENED ON 9 JULY 2026?

Current status: What happened on 9 July 2026? The extension of Chat Control 1.0 is **not yet formally law**. On 9 July 2026, the European Parliament examined the extension until 3 April 2028.

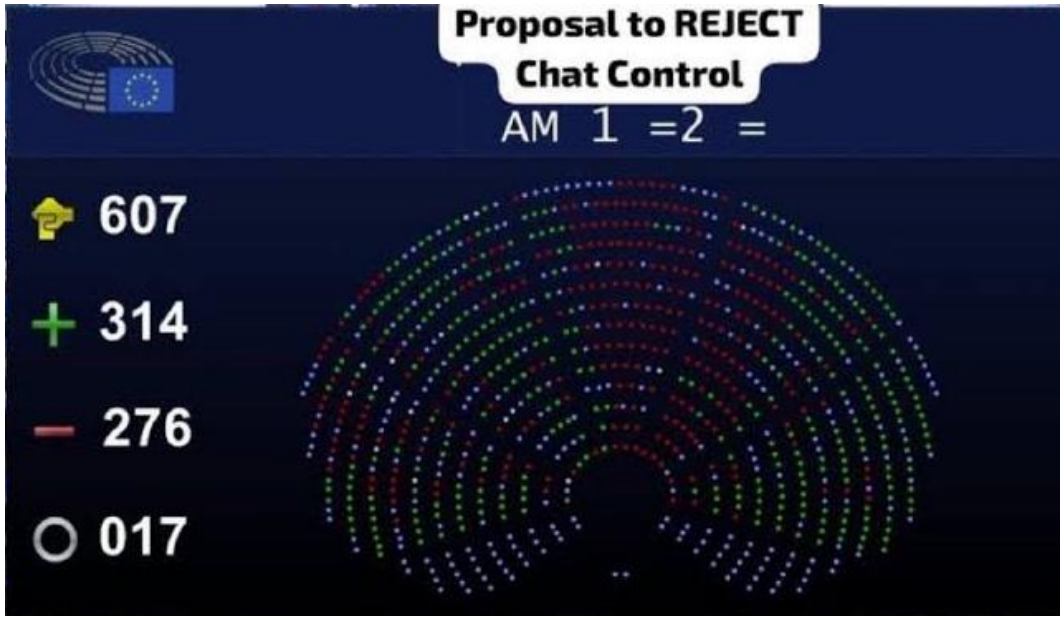
Although a majority of the MEPs present voted to reject it (314 against and 276 in favour), the objection failed. As this was a second reading, an absolute majority of the entire Parliament (361 votes) was required to block the text — a threshold that was not reached due to numerous absences before the summer recess.



The protection of encryption During the session, however, Parliament approved a crucial amendment: it explicitly excluded from the scope of monitoring all communications protected by end-to-end encryption (such as messages exchanged on WhatsApp, Signal or Telegram).

What happens now and the upcoming deadlines Since the text that emerged from Parliament was amended compared to the initial version, the legislative process is not yet complete:

- **Return to the Council**: The amended text has now been referred back to the Council of the European Union.
- **The three-month deadline**: The Council now has three months to decide how to proceed.
- **Approval or Conciliation (October 2026)**: If the Council accepts Parliament's amendment on encryption by autumn, the extension will become official law. If the Council rejects the amendment introduced by MEPs, a conciliation procedure between the two institutions will be opened to negotiate a common text.

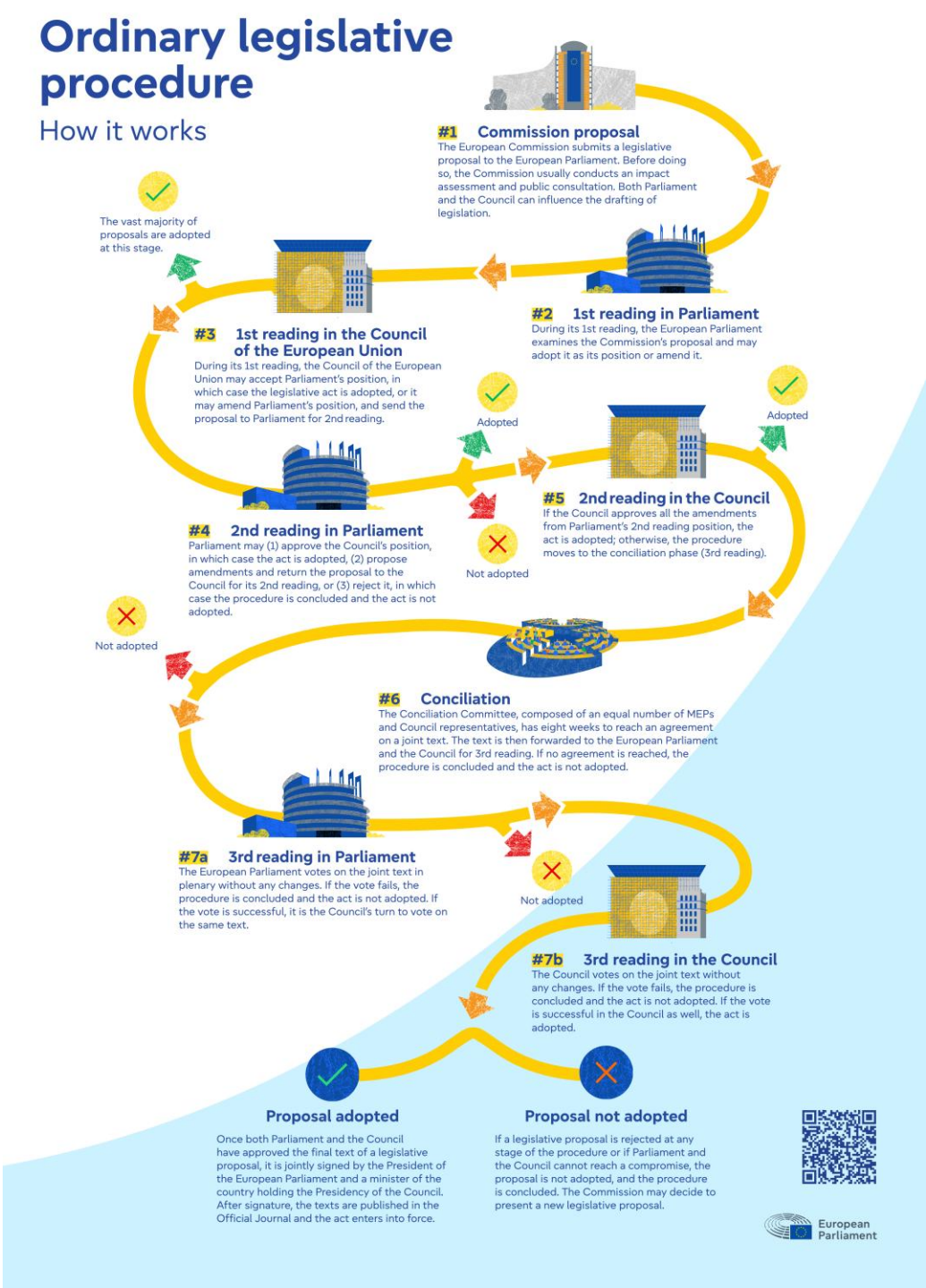


PART 2 – CAN CHAT CONTROL 1.0 BE REJECTED AND FAIL TO PASS SCRUTINY?

Yes, it can still be rejected. The ordinary European legislative procedure includes formal stages in which the text can be definitively blocked.

Rejection in the Council (second reading) The text amended by Parliament is now under examination by the Council of the EU. The Council can reject the act in two ways:

1) **Failure to agree on the amendments**: If the Council rejects Parliament's amendments (such as the protection of encryption), the text does not pass. A Conciliation Committee is automatically activated.
2) **Failure to achieve qualified majority**: If the required majority is not reached to approve the text (55% of Member States representing at least 65% of the EU population), the agreement collapses.
3) **Failure during the conciliation phase** If the Council does not approve Parliament's amendments, a direct negotiation phase (conciliation) begins, with a maximum duration of 6-8 weeks. If the Conciliation Committee does not reach agreement on a common text within the deadline, the act is definitively rejected and the procedure lapses.



Rejection in third reading If the Conciliation Committee reaches an agreement, the new common text must be voted on in third reading by both Parliament and the Council:

- **Vote in Parliament**: If the plenary rejects the common text by a simple majority of votes cast, the act lapses.
- **Vote in Council**: If the Council rejects the common text by qualified majority, the act is rejected.

In summary: The Council can cause the proposal to lapse by rejecting the compromises, or the text can fail due to lack of agreement in conciliation, or through a negative final vote in third reading.

Impact on users (for now) For users, nothing concrete changes at this stage: no new obligations are triggered, nor any form of mandatory scanning on devices. The measure simply reactivates the old voluntary derogation: platforms that were already carrying out voluntary checks (mainly on emails and non-end-to-end encrypted cloud services, such as certain Google or Meta services) can continue to do so. Chats and calls protected by end-to-end encryption remain completely excluded and intact. There is therefore no sudden “mass surveillance” on the most widely used messaging apps.

PART 3 – CHAT CONTROL 1.0 – THE BATTLE IS MORE OPEN AND UNCERTAIN THAN EVER

Now that Parliament has referred the extension of Chat Control 1.0 back to the Council with an absolute ban on touching encrypted chats (such as WhatsApp or Signal), the countries in favour will have to decide whether to yield to the requests of privacy defenders or risk blowing up the entire agreement during the conciliation phase.

The political context: a cross-party alliance against surveillance Opposition to Chat Control has created an unusual coalition that brings together groups that are normally far apart:

- **Greens/ALE** — the historical core of the resistance, denouncing procedural forcing and risks to fundamental rights.
- **Renew Europe (liberals)** — they led the key amendments to lock down end-to-end encryption.
- **Patriots for Europe and other right-wing/sovereigntist forces** — they co-signed the amendments to protect encryption.
- **The Left and much of the S&D group (Socialists)** — voted consistently against the extension (although some defections and absences in the Socialist group prevented reaching 361 votes).

On the other side, the EPP (European People's Party), the largest group, pushed for the urgency vote by taking advantage of the half-empty chamber before the summer recess. Together with the European Commission and several national governments in the Council, it supports the "protection of minors" line without sufficient guarantees on encryption.

By October/December, the Council will have to decide whether to accept this safeguard or risk collapsing the entire extension. **It is not yet law.**

Which Member States in the Council might oppose the amended extension? If the text amended by Parliament includes ironclad protection for WhatsApp and Signal, the countries that could obstruct and refuse to vote in favour in the Council are precisely the “hard-line” countries (those in favour of total control):

- **Spain**: the country that has been leading the push for years to gain access to all chats, including encrypted ones.
- **France and Denmark**: they have consistently exerted strong pressure not to limit the scanning powers of providers

Complete and clear Timeline of Chat Control in the EU

(updated as of 13 July 2026)

Date	Event	What happened
2020	Beginning	The European Commission proposes a temporary derogation from the ePrivacy Directive to allow platforms to continue voluntarily scanning chats for child sexual abuse material (CSAM), as new privacy rules would otherwise make this practice illegal.
14 July 2021	Birth of Chat Control 1.0	Regulation (EU) 2021/1232 is adopted. Temporary and voluntary derogation. Originally set to expire in August 2024. Only non-end-to-end encrypted services (Gmail, Facebook Messenger, Snapchat, Skype, iCloud, Xbox, etc.) use it.
May 2022	Birth of Chat Control 2.0	The Commission (Ylva Johansson) presents the permanent CSA Regulation proposal. It includes mandatory scanning obligations, detection orders, and the risk of client-side scanning even on encrypted messages. Strong opposition from experts, Parliament, EDPS and NGOs.
2023	Parliament	The European Parliament adopts a strong position: no mass scanning, no breaking of end-to-end encryption, only targeted judicial orders.
April 2024	First extension of 1.0	Chat Control 1.0 is extended until 3 April 2026.
2024–2025	Stalemate on 2.0	Four different Council Presidencies fail to find a majority for Chat Control 2.0. Germany and other countries block the harsher versions.
26 November 2025	Council	The Council finally adopts its negotiating position (Danish compromise): no mandatory detection orders, but risk-mitigation obligations and the possibility of “voluntary” scanning.
December 2025 – June 2026	Trilogues on 2.0	Trilogues begin (Parliament + Council + Commission). Five rounds of negotiations. No final agreement.
26 March 2026	Parliament rejects extension of 1.0	Parliament votes against further extension of Chat Control 1.0 (311 against, 228 in favour).
3–4 April 2026	Expiry of Chat Control 1.0	The derogation expires. Voluntary mass scanning becomes technically illegal. Some big companies (Google, Meta, Microsoft, Snap) declare they will continue anyway.
2 July 2026	Council	The Council adopts a “new” position that almost identically revives the expired derogation (via accelerated procedure).
7 July 2026	Parliament	Urgency procedure is approved (331–303).
9 July 2026	Return of Chat Control 1.0	Second-reading vote: 314 in favour of rejection, 276 against. Falls 47 votes short of the absolute majority of 361 → Chat Control 1.0 is revived until 3 April 2028. Amendment excluding end-to-end encryption is adopted.
July 2026 – today	Current situation	- Chat Control 1.0: in force until 2028 (pending formal Council approval). - Chat Control 2.0: still blocked, trilogues to resume in September 2026.

«What No One Is Saying: Big Tech Forced the Revival of Chat Control 1.0 on July 9 — After the April 3 Deadline Expired».

PHASE 1: The expiry and the “regulatory vacuum” (April 2026) The legal nature of the measure and the mechanism of “revival”

This is not a new law, but the “revival” of a temporary derogation from the **ePrivacy Directive (EU Regulation 2021/1232).**
This derogation temporarily suspends the obligation of confidentiality of communications imposed by the GDPR. In practice, it allows platforms to scan private content (emails, photos, non-encrypted messages) in search of child sexual abuse material (CSAM) without immediately violating the principle of secrecy of communications. The “revival” means that an existing norm that was due to expire is “brought back to life” through a technical renewal, without going through a full legislative process.

- The nature of the measure: This is not a new law, but the “revival” of a temporary derogation from the ePrivacy Directive (EU Regulation 2021/1232). This derogation temporarily suspends the obligation of confidentiality of communications imposed by the GDPR. In practice, it allows platforms to scan private content (emails, photos, non-encrypted messages) in search of child sexual abuse material (CSAM) without immediately violating the principle of secrecy of communications.
- The “revival” means that an existing norm that was due to expire is “brought back to life” through a technical renewal, without going through a full legislative process.

- The original expiry and the opening of the vacuum: On 26 March 2026, the European Parliament rejected the extension of the derogation. As a result, on 3 April 2026 the legal shield officially expired. From that moment onwards, any automatic scanning carried out on European servers became, from a legal point of view, an unlawful interception of private communications. This created a “regulatory vacuum” of about three months, during which the Big Tech companies were completely exposed.

- The operational and criminal dilemma of Big Tech: For about three months, giants such as Google, Meta, Microsoft and Snap lost their legal coverage. Continuing automatic scanning in Europe without this derogation would constitute a criminal and civil offence (unlawful interception of private communications), exposing them to multimillion-euro sanctions from Data Protection Authorities. The companies faced an impossible choice: turn off the filters and risk a major reputational disaster and accusations of failing to protect minors, or keep them on and risk criminal complaints and billion-euro fines.

REGULATION (EU) 2021/1232 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 14 July 2021

on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse

Article 1

Subject matter and scope

1. This Regulation lays down temporary and strictly limited rules derogating from certain obligations laid down in Directive 2002/58/EC, with the sole objective of enabling providers of certain number-independent interpersonal communications services ('providers') to use, without prejudice to Regulation (EU) 2016/679, specific technologies for the processing of personal and other data to the extent strictly necessary to detect online child sexual abuse on their services and report it and to remove online child sexual abuse material from their services.

2. This Regulation does not apply to the scanning of audio communications.

Article 2

Definitions

For the purposes of this Regulation, the following definitions apply:

(1) 'number-independent interpersonal communications service' means a number-independent interpersonal communications service as defined in Article 2, point (7), of Directive (EU) 2018/1972;

(2) 'online child sexual abuse material' means:

(a) child pornography as defined in Article 2, point (c), of Directive 2011/93/EU;

(b) pornographic performance as defined in Article 2, point (e), of Directive 2011/93/EU;

(3) 'solicitation of children' means any intentional conduct constituting a criminal offence under Article 6 of Directive 2011/93/EU;

(4) 'online child sexual abuse' means online child sexual abuse material and solicitation of children.

Article 3

Scope of the derogation

1. Articles 5(1) and 6(1) of Directive 2002/58/EC shall not apply to the confidentiality of communications involving the processing by providers of personal and other data in connection with the provision of number-independent interpersonal communications services provided that:

(a) the processing is:

(i) strictly necessary for the use of specific technology for the sole purpose of detecting and removing online child sexual abuse material and reporting it to law enforcement authorities and to organisations acting in the public interest against child sexual abuse and of detecting solicitation of children and reporting it to law enforcement authorities or organisations acting in the public interest against child sexual abuse;

(ii) proportionate and limited to technologies used by providers for the purpose set out in point (i);

(iii) limited to content data and related traffic data that are strictly necessary for the purpose set out in point (i);

(iv) limited to what is strictly necessary for the purpose set out in point (i);

(b) the technologies used for the purpose set out in point (a)(i) of this paragraph are in accordance with the state of the art in the industry and are the least privacy-intrusive, including with regard to the principle of data protection by design and by default laid down in Article 25 of Regulation (EU) 2016/679 and, to the extent that they are used to scan text in communications, they are not able to deduce the substance of the content of the communications but are solely able to detect patterns which point to possible online child sexual abuse;

(c) in respect of any specific technology used for the purpose set out in point (a)(i) of this paragraph, a prior data protection impact assessment as referred to in Article 35 of Regulation (EU) 2016/679 and a prior consultation procedure as referred to in Article 36 of that Regulation have been conducted;

(d) with regard to new technology, meaning technology used for the purpose of detecting online child sexual abuse material that has not been used by any provider in relation to services provided to users of number-independent interpersonal communications services ('users') in the Union before 2 August 2021, and with regard to technology used for the purpose of identifying possible solicitation of children, the provider reports back to the competent authority on the measures taken to demonstrate compliance with written advice issued in accordance with Article 36(2) of Regulation (EU) 2016/679 by the competent supervisory authority designated pursuant to Chapter VI, Section 1, of that Regulation ('supervisory authority') in the course of the prior consultation procedure;

(e) the technologies used are sufficiently reliable in that they limit to the maximum extent possible the rate of errors regarding the detection of content representing online child sexual abuse and, where such occasional errors occur, their consequences are rectified without delay;

(f) the technologies used to detect patterns of possible solicitation of children are limited to the use of relevant key indicators and objectively identified risk factors such as age difference and the likely involvement of a child in the scanned communication, without prejudice to the right to human review.

(g) the providers:

(i) have established internal procedures to prevent abuse of, unauthorised access to, and unauthorised transfers of, personal and other data;

(ii) ensure human oversight of and, where necessary, human intervention in the processing of personal and other data using technologies falling under this Regulation;

(iii) ensure that material not previously identified as online child sexual abuse material, or solicitation of children, is not reported to law enforcement authorities or organisations acting in the public interest against child sexual abuse without prior human confirmation;

(iv) have established appropriate procedures and redress mechanisms to ensure that users can lodge complaints with them within a reasonable timeframe for the purpose of presenting their views;

(v) inform users in a clear, prominent and comprehensible way of the fact that they have invoked, in accordance with this Regulation, the derogation from Articles 5(1) and 6(1) of Directive 2002/58/EC concerning the confidentiality of users' communications for the sole purpose set out in point (a)(i) of this paragraph, the logic behind the measures they have taken under the derogation and the impact on the confidentiality of users' communications, including the possibility that personal data are shared with law enforcement authorities and organisations acting in the public interest against child sexual abuse;

(vi) inform users of the following, where their content has been removed or their account has been blocked or a service offered to them has been suspended:

(1) the avenues for seeking redress from them;

(2) the possibility of lodging a complaint with a supervisory authority; and

(3) the right to a judicial remedy;

PHASE 2: The lobbying campaign and political pressure (April – June 2026)

- **The immediate industry reaction and the joint statement** Big Tech moved immediately to request a special derogation. On 4 April 2026, Google, Microsoft, Meta and Snap published an official joint statement entitled **“Reaffirming our commitment to child safety in the face of European Union inaction”**. The text was worded in such a way as to put European institutions with their backs to the wall, presenting the expiry of the derogation not as a legal problem for the companies, but as a political failure of the Union.

- **The strategy of pressure on the “security vacuum”** The companies, supported by NGOs such as Thorn, leveraged the “security vacuum”. Google (together with Meta, Microsoft and Snap) publicly declared in the statement “Reaffirming our commitment to child safety in the face of European Union inaction” that: “Today, because of the expiry of the ePrivacy derogation that allowed the use of technology to detect child sexual abuse material (CSAM), Europe risks leaving children less protected… we will continue to take voluntary action [even at the cost of legal risks]”. This wording serves to obtain criminal and contractual protection: the platforms continue to scan “voluntarily” and use the public statement to demonstrate their good faith and to exert political pressure. The message is clear: if Europe does not intervene, the blame for any abuses will fall on the institutions, not on the companies.

- **The surprise reopening of the dossier by Metsola** Under the weight of this media and political pressure, at the end of June the President of the European Parliament, Roberta Metsola, surprisingly reopened the institutional file and forwarded it to the Council of the EU. This was a move that unblocked a dossier that seemed closed, demonstrating how much the pressure from Big Tech and allied NGOs managed to change the political agenda in just a few weeks.

Reaffirming our commitment to child safety in the face of European Union inaction

Today, because of the expiry of the ePrivacy derogation enabling the use of technology to detect child sexual abuse material (CSAM), Europe risks leaving children across the globe less protected from the most abhorrent harm. This concern is shared by a group of almost 250 child rights organizations and many others.

For years, a number of technology companies have taken voluntary action to detect, remove and report CSAM including, where appropriate, through hash-matching technology — a widely utilized tool to prevent and disrupt real, ongoing harm to victims and survivors. This is not just a matter of law, but of protecting children.

While EU institutions rightly expect technology companies to take action on child safety, the April 3 expiry of the derogation clouds the legal certainty that has helped responsible platforms try to protect our communities, safeguard child victims, and preserve the integrity of our services. We are disappointed by this irresponsible failure to reach an agreement to maintain established efforts to protect children online.

As EU institutions continue to negotiate an immediate, interim solution and durable framework, signatory companies (Google, Meta, Microsoft, and Snap) reaffirm their continued commitment to protecting children and preserving privacy, and will continue to take voluntary action on our relevant Interpersonal Communication Services.

We call on EU institutions to conclude negotiations on a regulatory framework as a matter of urgency.

To learn more about how hash-matching and CSAM detection tools work, please join this upcoming webinar at 3PM CET on Friday, April 10th.

PHASE 3: The Council's procedural blitz and the default vote (July 2026)

The strategic change in voting rules (2 July) The Council of the EU (the governments of the 27 Member States) adopted the extension in the form of a "second-reading position". This strategic move, implemented just before the summer recess, upended the rules of the game: to reject the text, a simple majority of those present in the chamber was no longer enough; an absolute majority of all Members of the European Parliament (361 votes) was required. In this way, the Council made it much more difficult, if not impossible, to reject the measure during the holiday period.

Activation of the urgency procedure (7 July) A parliamentary urgency procedure was activated to bypass committee debate and bring the text directly to plenary session. This avoided in-depth examination and drastically reduced the time available for MEPs to analyse and challenge the measure.

The paradox of 9 July: majority of those present but absolute minority
The final vote took place on the last day before the summer recess:

- The majority of MEPs present in the chamber voted **AGAINST** the extension (314 votes against, 276 in favour);
- However, due to summer absences, the 314 votes against did not reach the required absolute majority threshold (361).

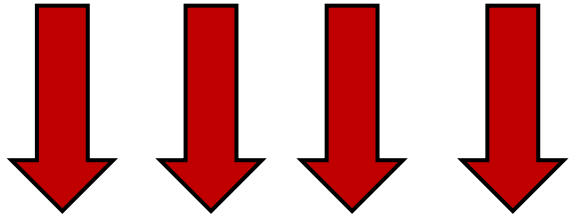
Result: due to a procedural loophole, the Council's position was approved by default. The derogation was extended ex officio until 3 April 2028. This was a "technical" vote that overrode the expressed will of the majority of those present.
The only parliamentary safeguard: the protection of end-to-end encryption The only safeguard approved by Parliament was a binding amendment that completely excludes communications protected by end-to-end encryption (such as WhatsApp and Signal) from scanning. This is the only point on which MEPs managed to obtain a concrete guarantee: apps that use point-to-point encryption remain outside the scope of the derogation.

PHASE 4: Application in contracts (ToS) and Content Policies

Explicit reference to the law as a legal shield To operate legally within this extension, Big Tech companies insert specific and coordinated clauses in their European documentation.
Explicit reference to the law: in the legal sections of Google and Meta (e.g., Safety Centre or Meta's legal pages), EU Regulation 2021/1232 is explicitly cited. This reference serves to demonstrate to the authorities that the scanning is neither arbitrary nor unilateral, but is solidly based on the renewed temporary derogation. Without this explicit reference, the activity would violate the principle of confidentiality of communications imposed by Europe.

Indemnity, implied consent and contractual protection: The Terms of Service (ToS) of non-encrypted services specify that by using the service, the user accepts the automated analysis of data for security purposes. In addition, companies contractually shield themselves from any legal actions brought by European users in the event of false positives (algorithm errors). In practice, the user implicitly accepts the scanning and waives, through contract, any recourse for possible system errors.

PHASE 5: How the authorised scanning works technically
Structured algorithmic surveillance, not human The mass surveillance authorised by the derogation does not involve direct human reading, but a structured algorithmic process. In developer guidelines and transparency reports, Google explains the exact technical steps that the derogation allows. In the guidelines, the commercial term "Chat Control" is never found, only explicit references to EU Regulation 2021/1232 or the Derogation from the ePrivacy Directive.



The derogation is not described as a “violation”, but as the necessary legal tool that allows engineers to keep the scanning servers active on EU territory.

1) Extraction of “Hashes” (Digital Fingerprints) When you receive or send an email on Gmail (or upload a file to Drive/Photos), a proprietary algorithm (or widely used tools such as Microsoft’s PhotoDNA) analyses multimedia files in transit on non-encrypted email or cloud and turns them into a unique string code called a “hash”. This process takes place in real time on central servers and is compared with international databases (NCMEC/IWF).

2) Comparison with international databases and AI analysis The hash code is compared in fractions of a second with international databases provided by organisations such as the National Center for Missing & Exploited Children (NCMEC) and the IWF. At the same time, AI systems analyse the pixels of images in search of nudity patterns and apply text scanning on clear-text chats to identify keywords related to grooming.

3) Precise scope of action Scanning takes place only on the central servers of non-end-to-end encrypted services. It includes: · Texts and attachments in Gmail and Outlook; · Files on Google Drive and Google Photos; · iCloud Mail; · Direct messages (DMs) on Instagram, Facebook Messenger, Snapchat, Discord and Skype.

4) Reporting (CyberTipline) and breach of correspondence secrecy If the algorithm finds an exact match (or a strong visual similarity via perceptual hashing), the 2021 derogation legally authorises Google (and other platforms) to breach correspondence secrecy, block the user’s account and forward the report to law enforcement via the NCMEC CyberTipline.

The political background: why Big Tech pushed so hard for the renewal

The three structural reasons for the lobbying pressure The major technology platforms (Google, Meta, Microsoft and Snap) were among the main lobbyists and promoters of the need to approve and renew this specific temporary extension. For them, the April 2026 expiry represented a huge legal and operational problem.
Here are the three key reasons:

1) **Fear of multimillion-euro sanctions (the criminal shield)**: Without the active derogation, the automatic scanning that these companies carry out on their servers (automatic filters on Gmail attachments or photos uploaded to Facebook) violates the European ePrivacy Directive. The companies faced an impossible choice: turn off the filters, risking enormous reputational damage and accusations of failing to protect minors; or keep them on, risking criminal complaints and billion-euro fines from European Data Protection Authorities for unlawful interception of private communications. The extension serves them first and foremost as a legal shield to continue operating with full legal certainty.
2) **Defence of their business model (Chat Control 1.0 vs 2.0)** There is a fundamental difference: · **Yes to Chat Control 1.0 (the current extension)**: the companies strongly support it because it allows voluntary controls managed by them, on their servers and on data that users upload in clear text. This does not affect the structure of their applications and does not force them to modify the clients. · **No to Chat Control 2.0 (the mandatory permanent proposal)**: the companies fiercely oppose the final proposal that would force them to scan phones (Client-Side Scanning). Companies like Meta (WhatsApp) or Signal have already stated that they would prefer to leave the European market rather than break the end-to-end encryption of their users.
3) **Coordinated media pressure and institutional guilt-tripping** As demonstrated by the joint statement of April 2026, the platforms used all their media influence to put pressure on the European Parliament. They leveraged the institutions' sense of guilt, warning that political deadlock would make Europe a "safe haven" for criminals due to the regulatory vacuum. This pressure pushed the most security-sensitive political groups (such as the EPP) to force the issue in July to unblock the situation, even at the cost of using procedural loopholes.

IN SUMMARY

The panic spreading on social media about the approval of Chat Control 1.0 is pure propaganda.

Not only is the text not yet law, but freedom of expression and the confidentiality of communications have already been heavily restricted for years.

Platforms like X (formerly Twitter) have long practiced constant censorship through shadowbans, reduced reach, account suspensions, and arbitrary algorithmic moderation.

What is being portrayed today as a future threat is already a daily reality carried out by the very same Big Tech companies that publicly opposed such laws while actively limiting users' freedom on their platforms.

Moreover, the issue remains completely open: nothing will be decided until October or December 2026, when the Council will determine whether to accept or reject the amendments.